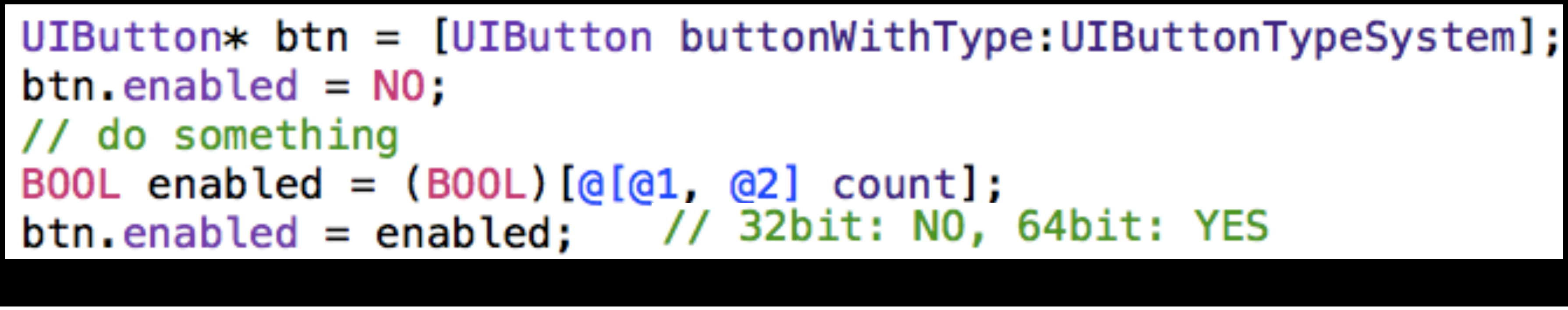
Daily Reverse

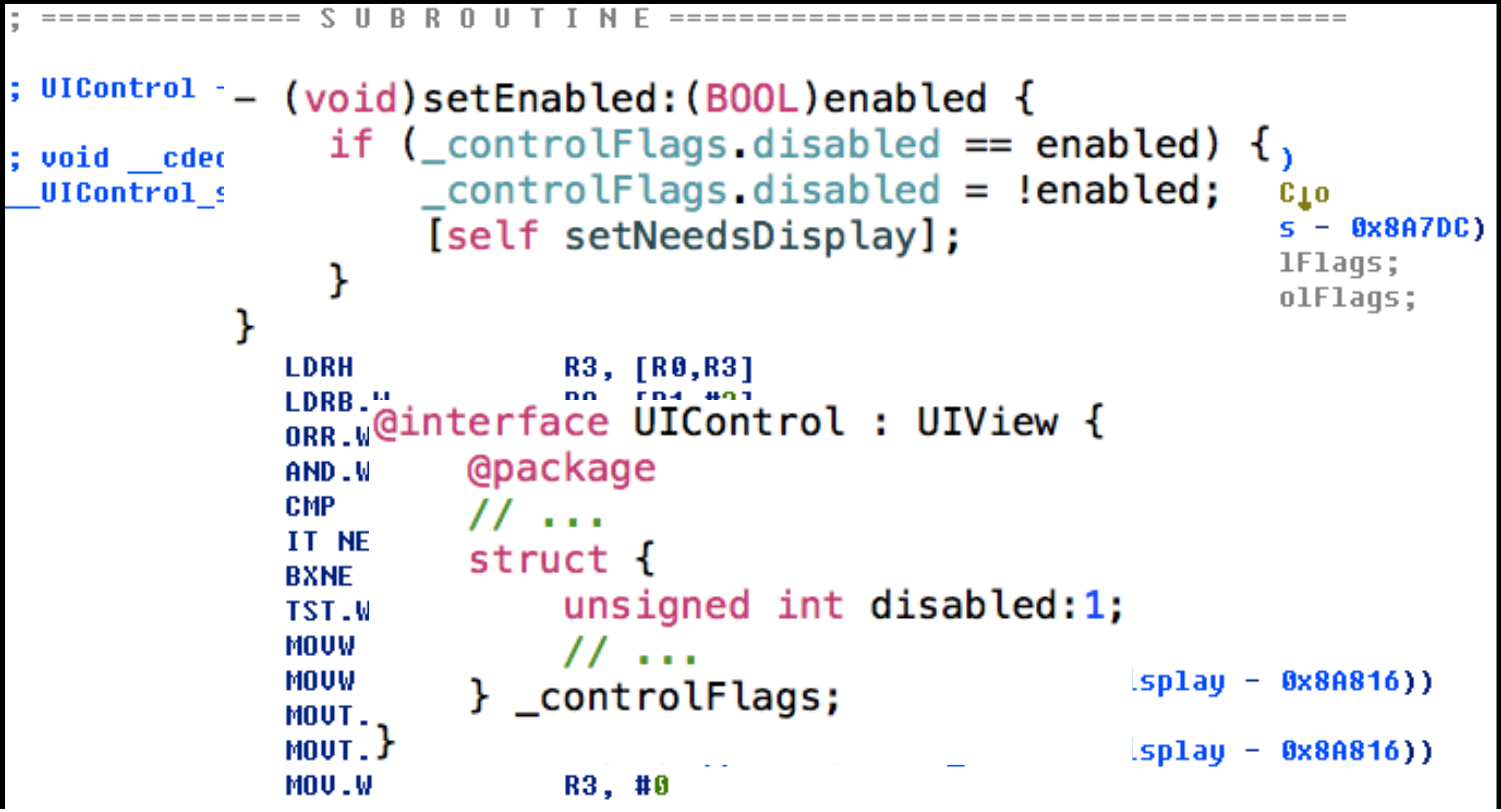
-- 逆向工程在iOS常规开发中的简单实践

- 为什么我们需要逆向?
- 逆向不都是越狱开发用的么?
- 如何应用逆向解决实际问题?
- 具体又如何实施?
- …..

逆向可以干什么?



```objc
UIButton* btn = [UIButton buttonWithType:UIButtonTypeSystem];
btn.enabled = NO;
// do something
BOOL enabled = (BOOL)[@[@1, @2] count];
btn.enabled = enabled;    // 32bit: NO, 64bit: YES
```



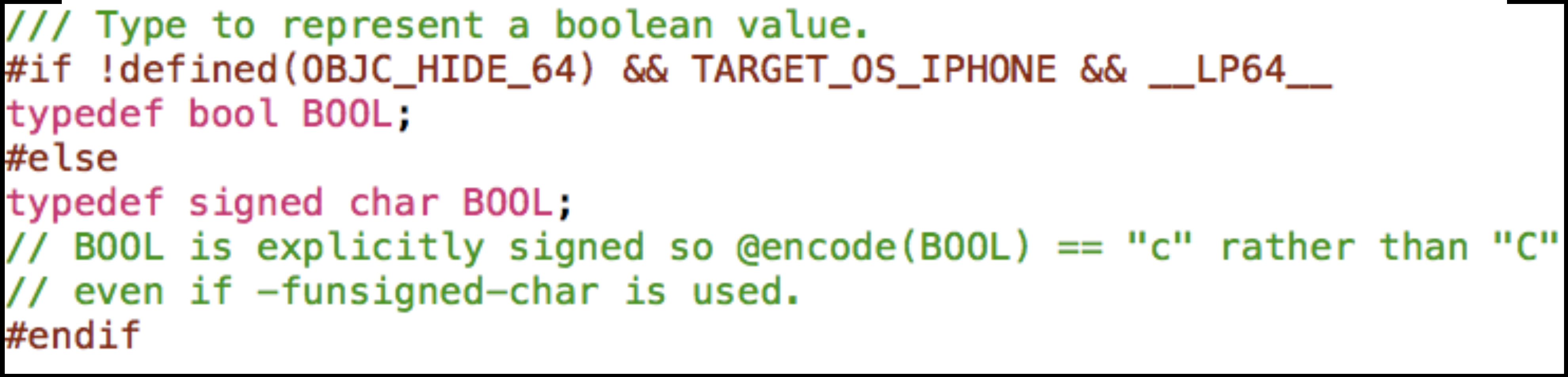
```
; =============== S U B R O U T I N E =======================================

; UIControl -
; void __cdec
__UIControl_s
```

```objc
- (void)setEnabled:(BOOL)enabled {
    if (_controlFlags.disabled == enabled) {
        _controlFlags.disabled = !enabled;
        [self setNeedsDisplay];
    }
}
```

```
LDRH            R3, [R0,R3]
LDRB.W
ORR.W
AND.W
CMP
IT NE
BXNE
TST.W
MOVW
MOVW
MOVT.
MOVT.
MOV.W           R3, #0
```

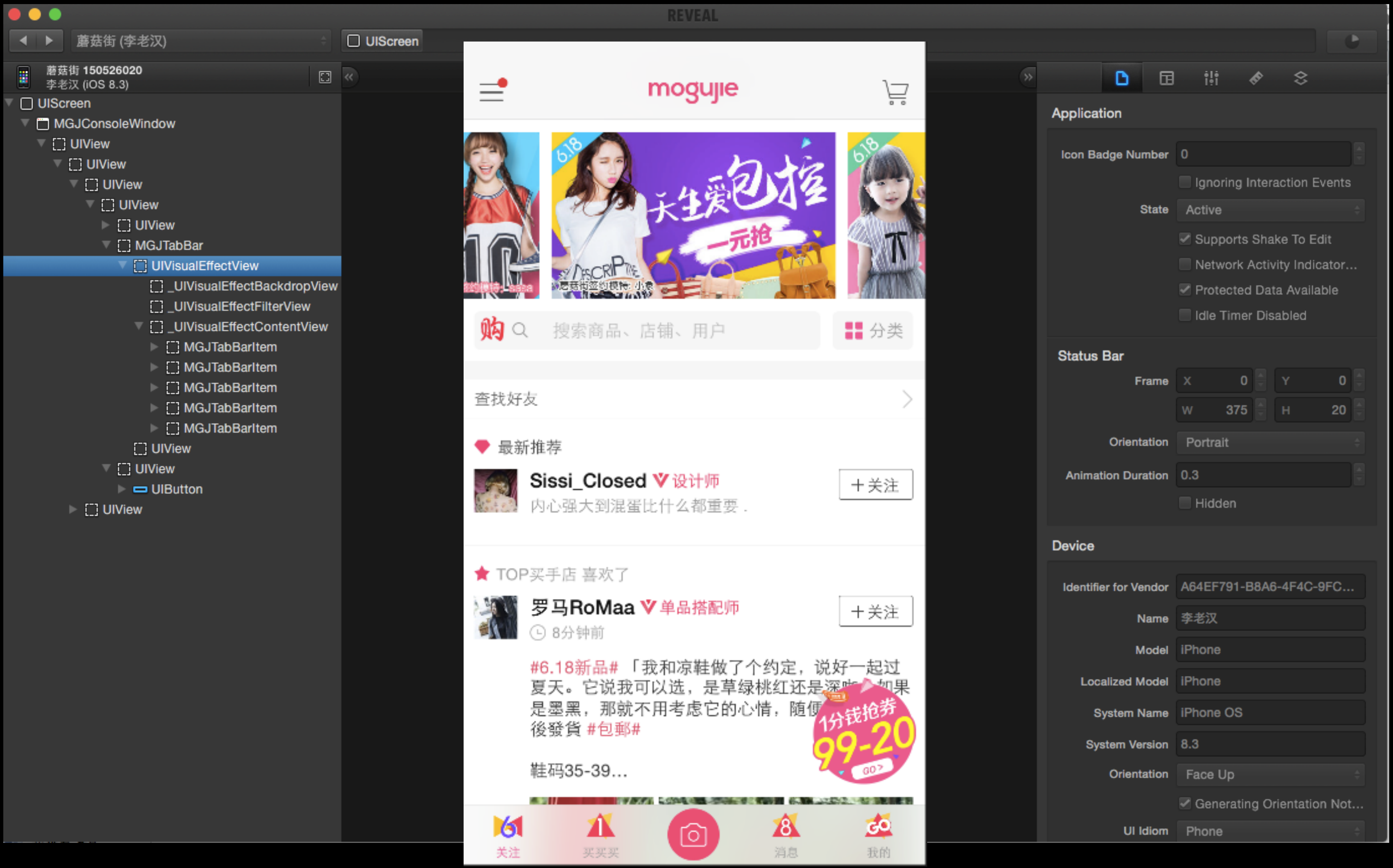
```
s - 0x8A7DC)
lFlags;
olFlags;
isplay - 0x8A816))
isplay - 0x8A816))
```

```objc
@interface UIControl : UIView {
    @package
    // ...
    struct {
        unsigned int disabled:1;
        // ...
    } _controlFlags;
}
```



```objc
/// Type to represent a boolean value.
#if !defined(OBJC_HIDE_64) && TARGET_OS_IPHONE && __LP64__
typedef bool BOOL;
#else
typedef signed char BOOL;
// BOOL is explicitly signed so @encode(BOOL) == "c" rather than "C"
// even if -funsigned-char is used.
#endif
```

示例二



```
▼ UIScreen
  ▼ MGJConsoleWindow
    ▼ UIView
      ▼ UIView
        ▼ UIView
          ▼ UIView
            ▶ UIView
            ▼ MGJTabBar
              ▼ UIVisualEffectView
                  _UIVisualEffectBackdropView
                  _UIVisualEffectFilterView
                ▼ _UIVisualEffectContentView
                  ▶ MGJTabBarItem
                  ▶ MGJTabBarItem
                  ▶ MGJTabBarItem
                  ▶ MGJTabBarItem
                  ▶ MGJTabBarItem
                UIView
            ▼ UIView
              ▶ UIButton
        ▶ UIView
```

查找好友

最新推荐

Sissi_Closed V 设计师

内心强大到混蛋比什么都重要 .

＋关注

TOP买手店 喜欢了

罗马RoMaa V 单品搭配师

8分钟前

＋关注

#6.18新品#「我和凉鞋做了个约定，说好一起过夏天。它说我可以选，是草绿桃红还是深咖 如果是墨黑，那就不用考虑它的心情，随便 後發貨 #包郵#

鞋码35-39...

Application

Icon Badge Number: 0

☐ Ignoring Interaction Events

State: Active

☑ Supports Shake To Edit

☐ Network Activity Indicator...

☑ Protected Data Available

☐ Idle Timer Disabled

Status Bar

Frame: X 0, Y 0, W 375, H 20

Orientation: Portrait

Animation Duration: 0.3

☐ Hidden

Device

Identifier for Vendor: A64EF791-B8A6-4F4C-9FC...

Name: 李老汉

Model: iPhone

Localized Model: iPhone

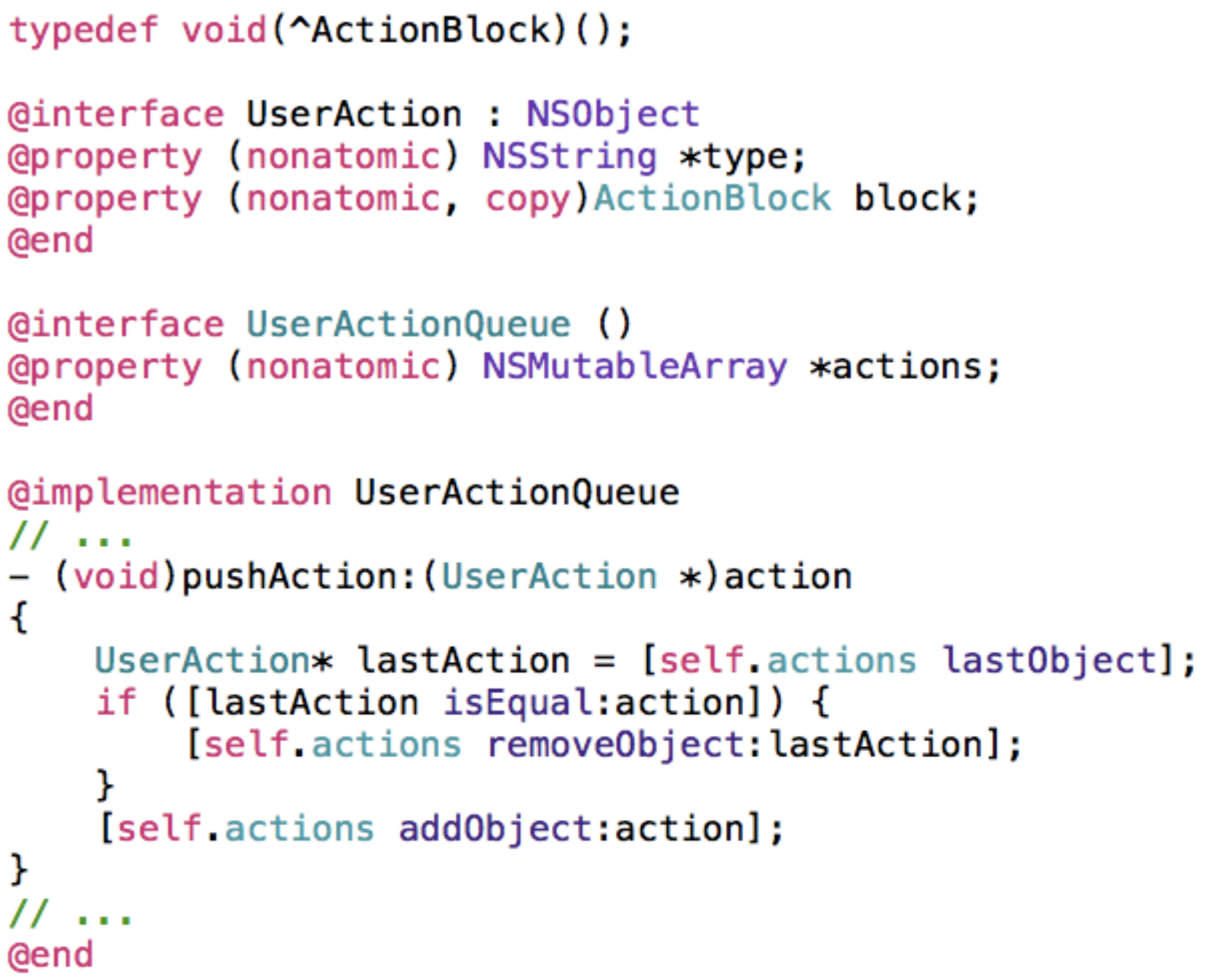
System Name: iPhone OS

System Version: 8.3

Orientation: Face Up

☑ Generating Orientation Not...

UI Idiom: Phone



```
typedef void(^ActionBlock)();

@interface UserAction : NSObject
@property (nonatomic) NSString *type;
@property (nonatomic, copy)ActionBlock block;
@end

@interface UserActionQueue ()
@property (nonatomic) NSMutableArray *actions;
@end

@implementation UserActionQueue
// ...
- (void)pushAction:(UserAction *)action
{
    UserAction* lastAction = [self.actions lastObject];
    if ([lastAction isEqual:action]) {
        [self.actions removeObject:lastAction];
    }
    [self.actions addObject:action];
}
// ...
@end
```

```
$ ./cycript -r 10.2.13.23:9426
```

```
cy# [x.type for each (x in queue)] // queue isKindOfClass UserActionQueue
["B","B","A"]

["B","A","B","A"] -> ["B","A","B","A"] + "A" -> ["B", "B", "A"]
```

逆向用来做什么

- 分析系统实现

-[UIButton setEnabled:]

- 分析第三方实现

UIVisualEffectView

- 分析自我实现

-[UserActionQueue pushQueue:]

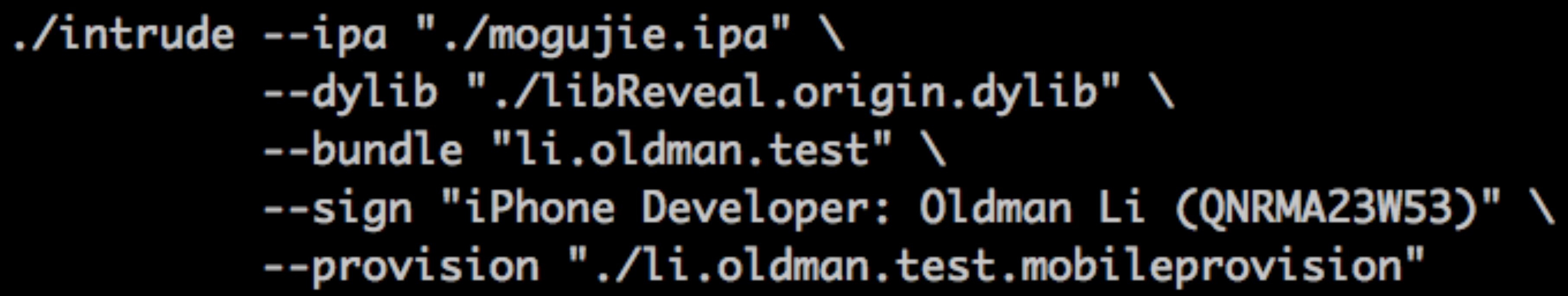
分析方法

- 离线分析
  - IDA Pro -[UIButton setEnabled:]
  - Class Dump
- 在线分析 Jailbreak
  - Reveal UIVisualEffectView
  - Cycript -[UserActionQueue pushQueue:]
  - LLDB

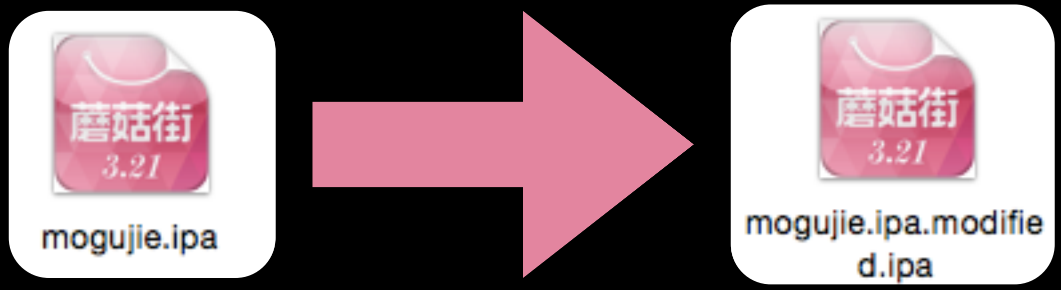
Jailbreak

- Difficulty: Rootless + iOS7/8/9 + Security
- Reason
- DYLD_INSERT_LIBRARIES

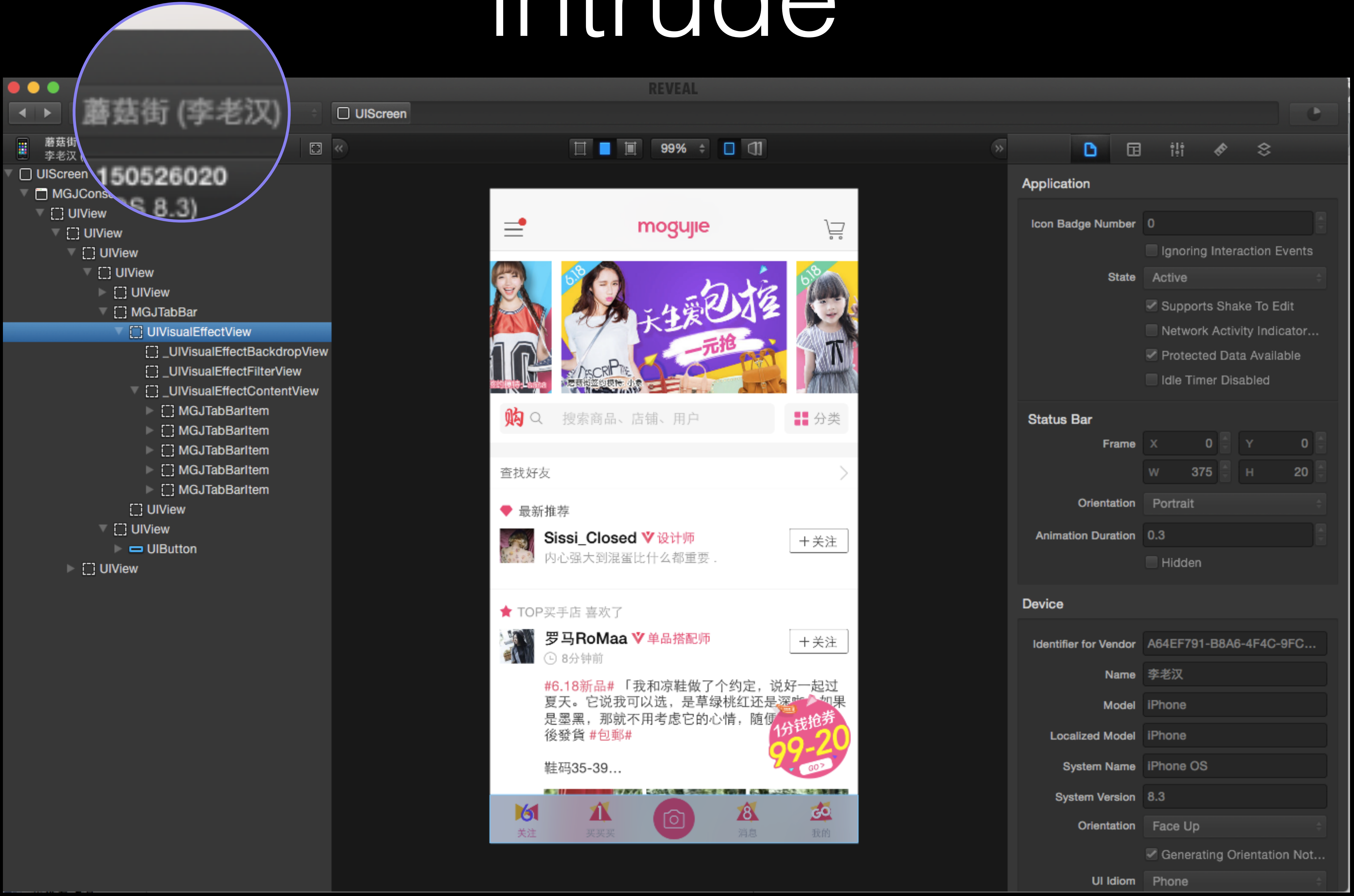
intrude



```
./intrude --ipa "./mogujie.ipa" \
          --dylib "./libReveal.origin.dylib" \
          --bundle "li.oldman.test" \
          --sign "iPhone Developer: Oldman Li (QNRMA23W53)" \
          --provision "./li.oldman.test.mobileprovision"
```



intrude



```
▼ UIScreen
  ▼ MGJCons…
    ▼ UIView
      ▼ UIView
        ▼ UIView
          ▼ UIView
            ▶ UIView
            ▼ MGJTabBar
              ▼ UIVisualEffectView
                  _UIVisualEffectBackdropView
                  _UIVisualEffectFilterView
                ▼ _UIVisualEffectContentView
                  ▶ MGJTabBarItem
                  ▶ MGJTabBarItem
                  ▶ MGJTabBarItem
                  ▶ MGJTabBarItem
                  ▶ MGJTabBarItem
                UIView
            ▼ UIView
              ▶ UIButton
        ▶ UIView
```

mogujie

购 搜索商品、店铺、用户 分类

查找好友

最新推荐

Sissi_Closed 设计师 +关注

内心强大到混蛋比什么都重要 .

TOP买手店 喜欢了

罗马RoMaa 单品搭配师 +关注

8分钟前

#6.18新品# 「我和凉鞋做了个约定，说好一起过夏天。它说我可以选，是草绿桃红还是深…如果是墨黑，那就不用考虑它的心情，随便…後發貨 #包郵#

鞋码35-39...

Application

Icon Badge Number: 0

□ Ignoring Interaction Events

State: Active

☑ Supports Shake To Edit

□ Network Activity Indicator...

☑ Protected Data Available

□ Idle Timer Disabled

Status Bar

Frame: X 0, Y 0, W 375, H 20

Orientation: Portrait

Animation Duration: 0.3

□ Hidden

Device

Identifier for Vendor: A64EF791-B8A6-4F4C-9FC...

Name: 李老汉

Model: iPhone

Localized Model: iPhone

System Name: iPhone OS

System Version: 8.3

Orientation: Face Up

☑ Generating Orientation Not...

UI Idiom: Phone

intrude

- 作用：给各种App嵌入各种Dylib
- 用途一：Reveal, Cycript, etc.
- 用途二：Jailbreak Tweaks
- 用途三：无侵入的自动化测试

intrude

https://github.com/imoldman/intrude

请善用逆向

Thanks!